ART 34 AMDT

Sub B1

New patent claims

1. A method for authenticating a smart card (*SIM*) in a messaging network, preferably a GSM network, wherein an algorithm and a secret key are stored in a smart card (*SIM*), whereby for authentication
   - the network or a network component first transfers a random number (*RAND*) to the smart card,
   - a response signal (*SRES*) is generated therefrom in the smart card by means of the algorithm and the secret key (K_i) and transmitted to the network or network component,

   characterized in that
   - to form the response signal (*SRES*) the secret key (K_i) and the random number (*RAND*) are each split into at least two parts (K_1, K_2; $RAND_1$, $RAND_2$),
   - one of the parts ($RAND_1$, $RAND_2$) of the transferred random number (*RAND*) is encrypted with the aid of one or more parts (K_1, K_2) of the secret key (K_i) by means of a one- or multistep, preferably symmetrical algorithm.
2. A method according to claim 1, characterized in that a given number of bits is selected from the encryption result and transferred as a signal response (*SRES*) to the network.
3. A method according to claim 1 ~~or 2,~~ characterized in that the secret key (K_i) and/or the random number (*RAND*) are split into two parts.
4. A method according to ~~any of claims 1 to 3~~ claim 1, characterized in that a part of the transferred random number (*RAND*) and one and/or more parts of the secret key (K_i) are used to calculate a channel coding key (K_c) by means of a one- or multistep algorithm, at least one part of the calculation result being used as the channel coding key (K_c).

5. A method according to ~~any of claims 1 to 4~~ claim 1, characterized in that the key (K_i) and the random number (*RAND*) are split into two equally long parts (K_1, K_2/ $RAND_1$, $RAND_2$).

6. A method according to ~~any of claims 1 to 5~~ claim 1, characterized in that DES algorithms are used to calculate the authentication parameters (*SRES*, *SRES'*) and/or the channel coding key (K_c).

7. A method according to ~~any of claims 1 to 5~~ claim 1, characterized in that the, preferably one-step, IDEA algorithm is used to calculate the authentication parameters (*SRES*, *SRES'*) and/or the channel coding key (K_c).

8. A method according to ~~any of claims 1 to 5,~~ claim 1 characterized in that a compression algorithm whose output value has a smaller length than the input parameter is used to calculate the authentication parameters (*SRES*, *SRES'*) and/or the channel coding key (K_c).

9. A method according to ~~any of claims 1 to 8~~ claim 1, characterized in that the calculation is effected in an at least two-step algorithm.

10. A method according to ~~any of claims 1 to 9,~~ claim 1 characterized in that a triple DES algorithm is used as an encryption algorithm, whereby one first encrypts with the first part (K_1) of the key (K_i), then decrypts with the second part (K_2) of the key (K_i) and thereupon encrypts again with the first part (K_1) or a third part of the key (K_i).

11. A method according to ~~any of claims 1 to 10~~ claim 1, characterized in that a selection of the first or second part of the random number (*RAND*) is effected in the same way in the card and the network in random or pseudorandom alternation.

T 18

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsbericht (Formblatt PCT/IPEA/416)
K 49 153/7 so		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Tag)*
PCT/EP99/02848	27/04/1999	07/05/1998
Internationale Patentklassification (IPK) oder nationale Klassifikation und IPK G07F7/10		
Anmelder GIESECKE & DEVRIENT GMBH et al.		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationale vorläufigen Prüfung beauftragte Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 7 Blätter einschließlich dieses Deckblatts.

   ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt 3 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Berichts
   - II ☐ Priorität
   - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderische Tätigkeit und der gewerbliche Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☐ Bestimmte angeführte Unterlagen
   - VII ☒ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☒ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
06/12/1999	13.07.00
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde: Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Burnes, K Tel. Nr. +49 89 2399 2393

Formblatt PCT/IPEA/409 (Deckblatt) (Januar 1994)

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP99/02848

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten.*):

Beschreibung, Seiten:

1-8 ursprüngliche Fassung

Patentansprüche, Nr.:

1-11 eingegangen am 03/05/2000 mit Schreiben vom 03/05/2000

Zeichnungen, Blätter:

1/2,2/2 ursprüngliche Fassung

2. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

☐ Beschreibung, Seiten:
☐ Ansprüche, Nr.:
☐ Zeichnungen, Blatt:

3. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)):

4. Etwaige zusätzliche Bemerkungen:

siehe Beiblatt

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1-11
	Nein:	Ansprüche	
Erfinderische Tätigkeit (ET)	Ja:	Ansprüche	
	Nein:	Ansprüche	1-11
Gewerbliche Anwendbarkeit (GA)	Ja:	Ansprüche	1-11
	Nein:	Ansprüche	

2. Unterlagen und Erklärungen

siehe Beiblatt

VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:

siehe Beiblatt

VIII. Bestimmte Bemerkungen zur internationalen Anmeldung

Zur Klarheit der Patentansprüche, der Beschreibung und der Zeichnungen oder zu der Frage, ob die Ansprüche in vollem Umfang durch die Beschreibung gestützt werden, ist folgendes zu bemerken:

siehe Beiblatt

I. Grundlage des Berichts

Ursprüngliche Offenbarung

1. Der geänderte unabhängige Anspruch 1 geht von der ursprünglichen Fassung des Anspruchs aus und wurde gegenüber dieser verallgemeinert, indem das letzte kennzeichnende Merkmal des ursprünglichen Anspruchs 1 (Auswahl von Bits aus dem Verschlüsselungsergebnis) weggelassen wurde und in einen neuformulierten abhängigen Anspruch (Anspruch 2 des geänderten Anspruchssatzes) überführt wurde.

   Diese Verallgemeinerung stützt sich auf die ursprüngliche Beschreibungsseite 6, Zeilen 24 bis 26, wo hervorgehoben ist, dass zur Bildung des Antwortsignals "auch nur Teile" aus dem Verschlüsselungsergebnis verwendet werden können, d.h. das Verschlüsselungsergebnis kann ganz oder teilweise verwendet werden.

2. Anspruch 2 des geänderten Anspruchssatzes beruht auf dem letzten kennzeichnenden Merkmal des ursprünglichen Anspruchs 1.

3. Die Ansprüche 3 bis 11 des geänderten Anspruchssatzes beruhen der Reihe nach auf den Ansprüchen 2 bis 10 des ursprünglichen Anspruchssatzes.

4. Der geänderte Satz von Ansprüchen beruht somit auf ursprünglicher Offenbarung und entspricht daher den Erfordernissen des Artikels 34 (2)b PCT.

Unterlagen und Erläuterungen zu Abschnitt V

Gewerbliche Anwendbarkeit, Neuheit und erfinderische Tätigkeit

5. Gewerbliche Anwendbarkeit im Sinn des Artikels 33 (4) PCT ist für die Verfahren nach den Ansprüchen 1 bis 11 offensichtlich gegeben.

6. Um den Bezug zum Stand der Technik klarer erörtern zu können, schickt der beauftragte Prüfer folgende Auslegung der Merkmale des Anspruchs 1 voraus.

Der unabhängige Anspruch 1 umfasst ein gattungsgemäßes Authentisierungsverfahren, bei dem

- der geheime Schlüssel (K_i) sowie die Zufallszahl (RAND) in jeweils wenigstens zwei Teile aufgeteilt werden und
- einer der Teile der Zufallszahl mit Hilfe des Schlüssels mittels eines Algorithmus verschlüsselt wird.

a) Zum ersten kennzeichnenden Merkmal des Anspruchs 1: Die Formulierung "in jeweils wenigstens zwei Teile aufgeteilt" umfasst den Fall, dass
- der Schlüssel aus zwei Teilen besteht, die zur Bildung des Antwortsignals als zwei Teile verwendet werden (mehr sagt der Anspruch über die Teilung des Schlüssels K_i nicht aus), und
- die Zufallszahl bereits in zwei Teilen übertragen wird (der Anspruch legt nicht fest, an welcher Stelle des Verfahrens die Teilung der Zufallszahl erfolgt).

b) Zum zweiten kennzeichnenden Merkmal des Anspruchs 1:
- Die Formulierung "mit Hilfe eines oder mehrerer Teile des geheimen Schlüssels verschlüsselt" umfasst eine Verschlüsselung mit Hilfe *aller* Teile des Schlüssels und somit mit Hilfe des (vollständigen) Schlüssels.
- Die Formulierung "mittels eines ein- oder mehrstufigen Algorithmus verschlüsselt" umfasst eine Verschlüsselung mittels jedweden Algorithmus (zB mittels einer mathematischen Funktion oder Funktionsgleichung).
- Die Formulierung "einer der Teile der Zufallszahl ... verschlüsselt wird" umfasst eine Verschlüsselung, bei der alle Teile der Zufallszahl verschlüsselt werden.

c) Anspruch 1 als Ganzer schließt nicht aus, dass Zufallszahlen und zugehörige Antwortsignale zwischen der Chipkarte und dem Netzwerk in *beiden* Richtungen übertragen werden.

7. Angesichts der vorstehend begründeten breiten Auslegbarkeit des Anspruchs 1 kommt das aus EP-A-0 098 437 (D3) bekannte Authentisierungsverfahren dem Verfahren nach Anspruch 1 nahe.

a) D3 ist einschlägig für die wechselseitige Authentifikation von Datenübertragungs-

partnern, wie aus der Beschreibungseinleitung der Entgegenhaltung (D3, zB Seite 3, Absatz 1) und der Klassifikation der Entgegenhaltung (G07F 7/08) deutlich wird. Deshalb berücksichtigt der Fachmann die in D3 angebotenen Lösungen, sobald er eine Authentifikationsaufgabe zu bewältigen hat.

b) Gemäß einer in D3 beschriebenen Ausführungsform (Tabelle II = Zeichnungsblatt 3/3; Seite 15, Zeile 24 ff) wird als Fragesignal eine Mehrzahl von Zufallszahlen (z_1 ... z_n) übertragen (Seite 16, Absatz 2), aus denen nacheinander (in m Zyklen) jeweils eine Gruppe entnommen und zu einer Rechengröße (x1; ...; xm) verknüpft wird (D3, Seite 17), was spätestens eine Aufteilung einer großen Zufallszahl darstellt (siehe Seite 6, Absatz 1 der vorliegenden Anmeldung), falls nicht schon die Übertragung der Mehrzahl von Zufallszahlen als Aufteilung anzusehen wäre.

c) Ferner nennt D3 als Beispiel für einen einfachen (einstufigen) Verschlüsselungsalgorithmus (die Funktionsgleichung y = x**(1/4) + 1,507 (Seite 13, Absatz 2). Darin können die numerischen Beispielswerte "4" und "1,507" als zwei Teile eines geheimen Schlüssels aufgefasst werden, den nur zwei authentische Kommunikationspartner kennen.

d) Schließlich kennt D3 auch schon das ("Verschleierungs"-)Prinzip, aus einem Verschlüsselungsergebnis nur ein Bruchstück zur weiteren Verwendung zu entnehmen (D3, Seite 4, Zeile 23 bis 32; Seite 13, Absatz 3), als zweite Stufe der Kodierung oder Verschlüsselung.

8. Vom Stand der Technik gemäß D3 unterscheidet sich das beanspruchte Verfahren somit in neuer Weise nur dadurch, dass es zur Authentisierung einer *Chipkarte* gegenüber einem Netzwerk verwendet wird.

Eine Verwendung von Authentisierungsverfahren zur Authentisierung von Chipkarten ist jedoch im Stand der Technik geläufig, siehe zB DE-A-34 26 006 (D4), Seite 4, Zeilen 14 bis 29.

Anspruch 1 erfüllt somit nicht die Erfordernisse des Artikels 33 (3) i.V.m. Regel 65 PCT, weil ein Verfahren mit den beanspruchten Schritten nicht auf erfinderischer Tätigkeit beruht.

9. Auch die zusätzlichen Merkmale der abhängigen Ansprüche stellen, soweit sie nicht ebenfalls unmittelbar durch den genannten Stand der Technik vorweggenommen sind, vom Fachmann zu erwartende Maßnahmen ohne überraschende Wirkung dar.

10. Nur der Vollständigkeit halber merkt der beauftragte Prüfer an, dass das erste und das zweite Dokument des europäischen Recherchenberichts dem Anmeldungsgegenstand offenbar nicht so nahe kommen wie D3.

a) EP-A-0 502 446 (D1) erwähnt zwar an drei Stellen (Spalte 2, Zeile 35; Spalte 3, Zeile 17; Spalte 4, Zeile 41) die Verwendung einer Zufallszahl zu Authentisierungszwecken, jedoch wird im dortigen Verfahren weder eine Zufallszahl noch ein Schlüssel geteilt.

b) Gemäß EP-A-0 840 480 (D2) wird zwar eine Zufallszahl geteilt und ein Schlüssel verwendet (s. zB die Zusammenfassung oder Spalte 5, Zeilen 9 bis 33), jedoch wird der Schlüssel nicht geteilt (sondern als Ganzes geändert, siehe Spalte 5, Zeilen 27 bis 33).

Abschnitt VII: Bestimmte Mängel der internationalen Anmeldung

11. In Zeile 19 des Anspruchs 1 hätte "werden" durch "wird" ersetzt werden sollen.

12. Um die Erfordernisse der Regel 5.1 (a) (ii) PCT zu erfüllen, hätten in der Beschreibungseinleitung die Druckschriften D3, D4 und D2 genannt und der darin enthaltene einschlägige Stand der Technik (siehe oben) kurz angegeben werden sollen.

Abschnitt VIII: Bestimmte Bemerkungen zur internationalen Anmeldung

13. Die Beschreibungseinleitung hätte an das geänderte Patentbegehren angepasst werden sollen (Regel 5.1 (a) (iii) PCT).

* * *

Neue Patentansprüche

1. Verfahren zur Authentisierung einer Chipkarte (SIM) in einem Netzwerk zur Nachrichtenübertragung, vorzugsweise in einem GSM-Netzwerk, bei dem in einer Chipkarte (SIM) ein Algorithmus sowie ein geheimer Schlüssel gespeichert sind, wobei zur Authentisierung
- zunächst vom Netzwerk oder einer Netzwerkkomponente eine Zufallszahl (RAND) an die Chipkarte übertragen wird,
- in der Chipkarte daraus mittels des Algorithmus und des geheimen Schlüssels (K_i) ein Antwortsignal (SRES) erzeugt und an das Netzwerk bzw. die Netzwerkkomponente übermittelt wird,
dadurch **gekennzeichnet**, daß
- zur Bildung des Antwortsignals (SRES) der geheime Schlüssel (K_i) sowie die Zufallszahl (RAND) in jeweils wenigstens zwei Teile (K_1, K_2; $RAND_1$, $RAND_2$) aufgeteilt werden,
- einer der Teile ($RAND_1$, $RAND_2$) der übertragenen Zufallszahl (RAND) mit Hilfe eines oder mehrerer Teile (K_1, K_2) des geheimen Schlüssels (K_i) mittels eines ein- oder mehrstufigen, vorzugsweise symmetrischen Algorithmus verschlüsselt werden.

2. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß eine vorgegebene Anzahl von Bits aus dem Verschlüsselungsergebnis ausgewählt und als Signalantwort (SRES) an das Netzwerk übertragen wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch **gekennzeichnet**, daß der geheime Schlüssel (Ki) und/oder die Zufallszahl (RAND) in zwei Teile aufgeteilt werden.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß ein Teil der übertragenen Zufallszahl (RAND) sowie ein und/oder weitere Teile des geheimen Schlüssels (Ki) zur Berechnung eines Kanalkodierungsschlüssels (K_c) mittels eines ein- oder mehrstufigen Algorithmus verwendet werden, wobei zumindest ein Teil des Berechnungsergebnisses als Kanalkodierungsschlüssel (K_c) verwendet wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß der Schlüssel (K_i) sowie die Zufallszahl (RAND) in zwei gleich lange Teile (K_1, K_2/$RAND_1$, $RAND_2$) aufgeteilt werden.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß zur Berechnung der Authentifizierungsparameter (SRES, SRES´) und/oder des Kanalkodierungsschlüssels (K_c) DES-Algorithmen verwendet werden.

7. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß zur Berechnung der Authentisierungsparameter (SRES, SRES´) und/oder des Kanalkodierungsschlüssels (K_c) der, vorzugsweise einstufige, IDEA-Algorithmus verwendet wird.

8. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß zur Berechnung der Authentisierungsparameter (SRES, SRES´) und/oder des Kanalkodierungsschlüssels (K_c) ein Komprimierungsalgorithmus verwendet wird, dessen Ausgabewert eine geringere Länge als der Eingabeparameter aufweist.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch **gekennzeichnet**, daß die Berechnung in einem mindestens zweistufigen Algorithmus erfolgt.

10. Verfahren nach einem der Ansprüche 1 bis 9, dadurch **gekennzeichnet**, daß als Verschlüsselungsalgorithmus ein Triple-DES-Algorithmus verwendet wird, bei dem zunächst mit dem ersten Teil (K_1) des Schlüssels (K_i) verschlüsselt, anschließend mit dem zweiten Teil (K_2) des Schlüssels (K_i) entschlüsselt und darauf wieder mit dem ersten Teil (K_1) oder einem dritten Teil des Schlüssels (K_i) verschlüsselt wird.

11. Verfahren nach einem der Ansprüche 1 bis 10, dadurch **gekennzeichnet**, daß eine Auswahl des ersten oder zweiten Teils der Zufallszahl (RAND) im zufälligen oder pseudozufälligen Wechsel in der Karte und im Netzwerk in gleicher Weise erfolgt.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AUF DEM GEBIET DES PATENTWESENS

E.K.

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
K 49 153/7ch			
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)*	
PCT/EP 99/ 02848	27/04/1999	07/05/1998	
Anmelder			
GIESECKE & DEVRIENT GMBH			

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1

   [ ] wie vom Anmelder vorgeschlagen [ ] keine der Abb.

   [X] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 99/02848

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G07F7/10

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 G07F G07C E05B H04L H04Q

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 502 446 A (SIEMENS AG) 9. September 1992 (1992-09-09) das ganze Dokument ---	1,3
A	EP 0 840 480 A (MATSUSHITA ELECTRIC IND CO LTD ;TOKYO SHIBAURA ELECTRIC CO (JP)) 6. Mai 1998 (1998-05-06) Zusammenfassung; Abbildungen 3,7 Spalte 3, Zeile 44 - Spalte 5, Zeile 38 Spalte 7, Zeile 49 - Spalte 13, Zeile 25 ---	1
A	EP 0 098 437 A (HUELSBECK & FUERST) 18. Januar 1984 (1984-01-18) Zusammenfassung; Abbildungen Seite 9, Zeile 15 - Seite 18, Zeile 6 --- -/--	1

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
23. August 1999	31/08/1999

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Buron, E

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 34 26 006 A (PHILIPS NV) 7. Februar 1985 (1985-02-07) Zusammenfassung; Abbildung 1 Seite 4, Zeile 1 - Seite 9, Zeile 30	1

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 99/02848

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0502446 A	09-09-1992	AT 145511 T	15-12-1996
		DE 59207527 D	02-01-1997
		ES 2095339 T	16-02-1997
EP 0840480 A	06-05-1998	CN 1215271 A	28-04-1999
		JP 10233771 A	02-09-1998
EP 0098437 A	18-01-1984	DE 3225754 A	12-01-1984
		JP 1689338 C	11-08-1992
		JP 3058031 B	04-09-1991
		JP 59048567 A	19-03-1984
		US 4509093 A	02-04-1985
DE 3426006 A	07-02-1985	FR 2549989 A	01-02-1985
		GB 2144564 A,B	06-03-1985
		JP 1706001 C	27-10-1992
		JP 3074432 B	26-11-1991
		JP 60049471 A	18-03-1985
		SE 460157 B	11-09-1989
		SE 8403867 A	30-01-1985
		US 4612413 A	16-09-1986

09673658

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

10

Applicant's or agent's file reference K 49 153/7 so	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/EP99/02848	International filing date (*day/month/year*) 27 April 1999 (27.04.99)	Priority date (*day/month/year*) 07 May 1998 (07.05.98)
International Patent Classification (IPC) or national classification and IPC G07F 7/10		
Applicant GIESECKE & DEVRIENT GMBH		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 3 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
06 December 1999 (06.12.99)	13 July 2000 (13.07.2000)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/EP99/02848

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☐ the international application as originally filed.

☒ the description, pages 1-8, as originally filed,
pages _____, filed with the demand,
pages _____, filed with the letter of _____,
pages _____, filed with the letter of _____.

☒ the claims, Nos. _____, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1-11, filed with the letter of 03 May 2000 (03.05.2000),
Nos. _____, filed with the letter of _____.

☒ the drawings, sheets/fig 1/2,2/2, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

See supplemental sheet.

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-11	YES
	Claims		NO
Inventive step (IS)	Claims		YES
	Claims	1-11	NO
Industrial applicability (IA)	Claims	1-11	YES
	Claims		NO

2. Citations and explanations

5. Industrial applicability (PCT Article 33(4)) is clearly established for the method according to Claims 1 to 11.

6. To be able to discuss more clearly how the invention relates to the prior art, we must interpret the features of Claim 1 as follows.

Independent Claim 1 comprises a generic authentication method in which
- the secret key (K_i) and the random number (RAND) are each divided into at least two parts and
- one of the parts of the random number is encoded by an algorithm with the help of the key.

a) Re. the first characterising feature of Claim 1:
The wording "each divided into at least two parts" encompasses the following cases:
- the key consists of two parts used to form the reply signal as two parts (the claim says nothing further as to the division of the key K_i), and
- the random number is already transmitted in two parts (the claim does not specify at which point in the process the division takes place).

b) Re. the second characterising feature of Claim 1:
- the wording "encoded with the help of one or more parts of the key" encompasses an encoding with the help of *all* parts of the key and thus with the help of the (complete) key;
- the wording "encoded by a single or multi-step algorithm" encompasses an encoding by any algorithm (for example, by a mathematical function or functional equation);
- the wording "one of the parts of the random number ... is encoded" encompasses an encoding in which all the parts of the random number are encoded.

c) Claim 1 as a whole does not exclude the possibility that random numbers and corresponding reply signals are transmitted between the chip card and the network in *both* directions.

7. Given that Claim 1 can be interpreted in the broad manner detailed above, the authentication method known from EP-A-0 098 437 (D3) is closest to the method according to Claim 1.

a) D3 is relevant to the reciprocal authentication of data transmission partners, as is clear from the introductory part of the description of said citation (D3, for example, page 3, paragraph 1) and from the classification of said citation (G07F 7/08). Therefore, a person skilled in the art would take D3 into consideration if he were addressing the problem of authentication.

b) As per an embodiment described in D3 (Table II = drawings sheet 3/3; page 15, lines 24ff.), most of

the random numbers (z_1 ... z_n) are transmitted as an interrogation signal (page 16, paragraph 2) from each of which (in m cycles) a group is successively extracted and linked to form an operand (x1; ...; xm) (D3, page 17), which ultimately constitutes a division of a large random number (see page 6, paragraph 1 of the present application), assuming that the transmission of most of the random numbers were not already considered to be such a division.

c) Furthermore, as an example of a simple (single-step) encoding algorithm, D3 gives the functional equation y = x**(1/4) + 1.507 (page 13, paragraph 2). The numeric values "4" and "1.507" in the example can be considered as two parts of a secret key known only to two authentic communication partners.

d) Finally, D3 also already describes the ("masking") principle of deriving from an encoded product only a fragment for further use (D3, page 4, lines 23 to 32; page 13, paragraph 3), as the second step of the coding or encoding.

8. Thus, the claimed method differs in a novel way from the prior art as per D3 only in that it is used to authenticate a *chip card* in a network.

However, authenticating chip cards with an authentication method is a standard measure in the prior art - see, for example, DE-A-34 26 006 (D4), page 4, lines 14 to 29.

Therefore, Claim 1 does not meet the requirements of PCT Article 33(3) in conjunction with PCT Rule 65, because a method with the claimed steps does not

involve an inventive step.

9. Furthermore, the additional features of the dependent claims, insofar as they are not likewise anticipated directly by the prior art, are measures that one would expect from a person skilled in the art and which have no surprising effect.

10. For the sake of completeness, it should be noted that the first and second documents in the European search report are clearly not as closely related to the subject matter of the application as D3.

a) Although EP-A-0 502 446 (D1) mentions in three places (column 2, line 35; column 3, line 17; column 4, line 41) using a random number for authentication purposes, neither a random number nor a key is divided in the methods in said document.

b) Although, as per EP-A-0 840 480 (D2), a random number is divided and a key is used (see, for example, the abstract or column 5, lines 9 to 33), the key is not divided (but is altered as a whole - see column 5, lines 27 to 33).

I. Basis of the report

1. This report has been drawn on the basis of *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.)*:

4. Original disclosure

1. The amended independent Claim 1 is based on the original version of the claim and is a more general version thereof, in that the final characterising feature of the original Claim 1 (the selection of bits from the encoding result) has been removed and included instead in a redrafted dependent claim (Claim 2 of the amended set of claims).

This generalisation is supported by page 6, lines 24 to 26, of the original description, which emphasises the fact that, to form a reply signal, "even just portions" of the encoded data can be used, that is, the encoded data can be used as a whole or in part.

2. Claim 2 of the amended set of claims is based on the final characterising feature of the original Claim 1.

3. Claims 3 to 11 of the amended set of claims are based, in sequence, on Claims 2 to 10 of the original set of claims.

4. The amended set of claims is thus based on the original disclosure and consequently meets the requirements of PCT Article 34(2)(b).

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

11. In line 19 of Claim 1, (the verb in the plural) "are" should have been "is".

12. Pursuant to PCT Rule 5.1(a)(ii), the introductory part of the description should have cited publications D3, D4 and D2 and should have briefly outlined the relevant prior art (see above) contained therein.

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

13. The introductory part of the conclusion should have been brought into line with the amended claims.